Amendment to the Claims:

The listing of claims will replace all prior versions, and listings of claims in the application:

Listing of Claims:

1. (Currently Amended) A method for preventing unauthorized use of software accessing at least one specific hardware module comprising a unique hardware identification sequence wherein said software comprises a license key for being executed, comprising:

[-] reading out said hardware identification sequence of said at least one specific hardware module~~,~~;

[-] retrieving a predetermined hardware identification sequence contained in said license key~~,~~

[-] comparing said read-out hardware identification sequence with said hardware identification sequence contained in the license key; ~~and~~

[-] permitting execution of said software if both sequences match~~,~~; and wherein

said hardware identification sequence contained in said license key is encrypted and a secret key coded in said software is used to decrypt said hardware identification sequence.

2-5. Cancelled (without disclaimer or prejudice).

6. (Currently Amended) The method according to claim ~~5~~22, wherein said public key is encrypted additionally using a public key encryption method, comprising:

[-] a second secret key which is only known to a trusted third authority; and

[-] a second public key corresponding to said second secret key~~,~~; and

wherein said second secret key is used for encrypting said public key and said second public key is used for decrypting said encrypted public key and wherein said second public key is the only key which allows ~~to~~ decrypting data encrypted by the second secret key.

7. Cancelled (without disclaimer or prejudice).

8. (Currently Amended) The method according to ~~anyone of the preceding~~ claims 1, 7, 21 and 22, wherein at least one of said specific hardware modules is a network interface module comprising a unique network interface address ~~(MAC)~~.

9. (Currently Amended) The method according to claim 8, wherein at least one of said specific hardware modules is a Bluetooth[™] module comprising a unique Bluetooth[™] hardware address.

10-16. Cancelled (without disclaimer or prejudice).

17. (Currently Amended) The method according to claim ~~4~~21, wherein at least one of said specific hardware modules is a network interface module comprising a unique network interface address ~~(MAC)~~.

18. (Currently Amended) The method according to claim ~~5~~22, wherein at least one of said specific hardware modules is a network interface module comprising a unique network interface address ~~(MAC)~~.

19. (Currently Amended) The method according to claim 6, wherein at least one of said at least one specific hardware modules is a network interface module comprising a unique network interface address ~~(MAC)~~.

20. (Currently Amended) The method according to claim 7, wherein at least one of said at least one specific hardware modules is a network interface module comprising a unique network interface address ~~(MAC)~~.

21. (New) A method for preventing unauthorized use of software accessing at least one specific hardware module comprising a unique hardware identification sequence wherein said software comprises a license key for being executed, comprising:

reading out said hardware identification sequence of said at least one specific hardware module;

retrieving a predetermined hardware identification sequence contained

in said license key;

comparing said read-out hardware identification sequence with said hardware identification sequence contained in the license key;

permitting execution of said software if both sequences match; and wherein

said hardware identification sequence contained in said license key is encrypted and a secret algorithm coded in said software is used to decrypt said hardware identification sequence.

22. (New) A method for preventing unauthorized use of software accessing at least one specific hardware module comprising a unique hardware identification sequence wherein said software comprises a license key for being executed, comprising:

reading out said hardware identification sequence of said at least one specific hardware module;

retrieving a predetermined hardware identification sequence contained in said license key;

comparing said read-out hardware identification sequence with said hardware identification sequence contained in the license key;

permitting execution of said software if both sequences match; and

said hardware identification sequence contained in said license key is encrypted and a public key encryption method is used for encrypting and decrypting said unique hardware identification sequence contained in said license key,

comprising a secret key which is only known to the license key distribution authorities; and a public key corresponding to said secret key; and wherein

said secret key is used for encrypting said hardware identification sequence and said public key is used for decrypting said hardware identification sequence and wherein said public key is the only key which allows decrypting data encrypted by the secret key.